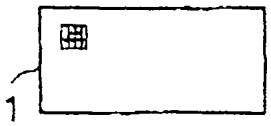
Transaction request



TERMINAL 3

Server
(e.g. banking)

dti

Security procedure
CT
CA

MESSAGE (1)

transaction request (e.g. payment)
(cryptogram MAC1 (CT))
Transaction

CT
CA

MESSAGE (2)

Response to the transaction including action request (n actions=script 1)

(loading command)
cryptogram MAC2
script 1

CA'=CA+n

MESSAGE (3)

Acknowledgement

MAC3
CA'

Verification MAC3
Verification CA'=CA+n

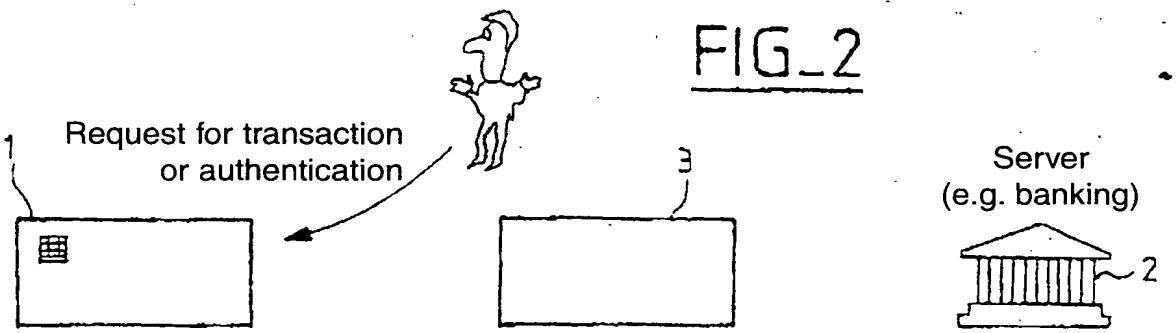
MESSAGE (4)

dtj

Request for new transaction
MAC'1 (CT')
Transaction
CA

FIG_1

FIG_2



Application
- Calculation of card authentication data MAC1.
Reading of action counter CA

MESSAGE ①

Transaction request
- MAC1
- CA
- Banking transaction

- Verification MAC1
- Performs the transaction
- Calculation of server authentication data MAC2
- Preparation of command for changing parameter of script 1
- Storage of CA and script 1 in DB server

E.g. line cut off

MESSAGE ②

Response to transaction including action request (script 1)

{loading command
MAC2, script 1)

MESSAGE ③

New transaction request

{- MAC1, CA
- Banking transaction

Application
- Calculation of card authentication data MAC1
- Reading of action counter CA

- Verification of MAC1
- Verification of CA_{card} = CA_{server} ⇨ cancels last transaction
- Calculation of MAC2
- Preparation of new script 2
Storage CA' and script 2 in DB server

MESSAGE ④

Response to transaction including action request (script 2)

{Loading command
MAC 2, script 2

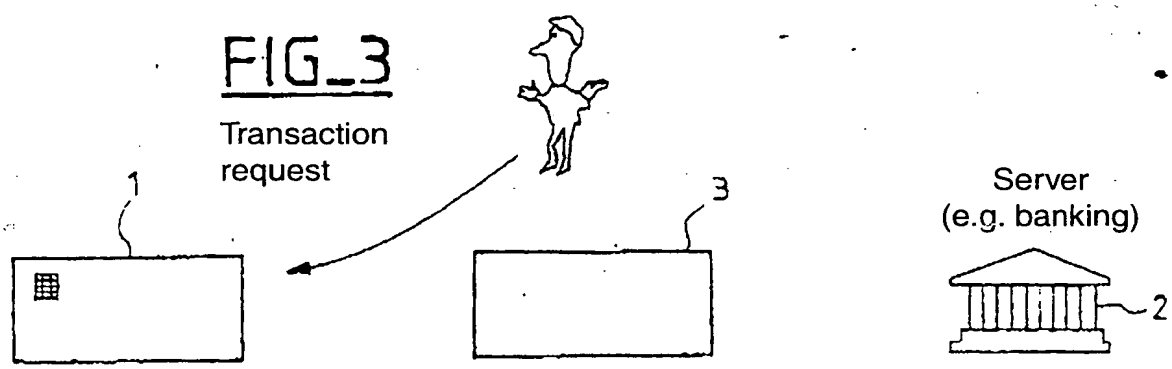
- Verification of MC2
- If MAC2 OK then effect script 2#
- If script 1 OK, incrementation CA=CA+1
- Calculation of acknowledgement MAC3

MESSAGE ⑤

Acknowledgement
MAC 3, CA+1

- Verification MAC 3
- Verification CA'=CA+1
- Erasure of DB

FIG_3



Application
- Calculation of card authentication data MAC1.
- Reader for action counter CA

MESSAGE (1)

Transaction request
- MAC1
- CA
- Banking transaction

- Verification of MAC1
- Effects transaction
- Calculation of server authentication data MAC2
- Preparation of change in parameter command script 1
- Storage of CA and script in DB server

MESSAGE (2)

Response to transaction including action request (script 1)
{ Loading command
MAC2, script 1

- Verification of MAC2
- if MAC 2 OK then effect script 1
- if script 1 OK incrementation CA'=CA+1
- Calculation of acknowledgement MAC3

MESSAGE (3) (e.g. line cutoff)

Acknowledgement

MESSAGE (4)

Application
- Calculation of card authentication data MAC1
- Reading of action counter CA'=CA+n

New action request
- MAC1, CA'
- Banking transaction

- Verification of MAC1
- Verification
- CA' $_{card}$=CA+n last transaction OK
- Effects current transaction
- Calculation MAC2
- Preparation new script 2
- Storage CA' in script 2 in DB server

MESSAGE (5)

Response to transaction including action request (script 2)
{ Loading command
MAC2, script 2

- Verification MC2
- if MAC2 OK then effects script 2
- if script 1 OK, incrementation CA'=CA'+1
- Calculation of acknowledgement MAC3

MESSAGE (6)

Acknowledgement
MAC3, CA'

- Verification MAC3
- Verification of CA'=CA'+1
- Erasure of DB